BLANKROME

Cybersecurity and Intellectual Property

APRIL 6, 2020 • NO. 1

Zoombombing Security & Privacy: Lessons from Zoom's Recent Conduct

The outbreak of the coronavirus ("COVID-19") pandemic in the United States has, with astounding speed, shifted much of America's workforce to remote status. Videoconferencing apps like Zoom have surged, but so have security and data privacy concerns. Zoom's recent circumstances provide important lessons for tech companies dealing with the tremendous shift to remote work.

Despite its recent success, Zoom is now scrambling to address security and data privacy concerns with its popular video conferencing app. Over the past few weeks, Internet trolls and consumer advocacy groups alike have highlighted vulnerabilities with Zoom's technology, including one that enables uninvited guests to hijack Zoom's screen-sharing feature during meetings—now dubbed "Zoombombing." Consumer advocacy groups have also raised alarms over Zoom's undisclosed sharing of users' private information with third parties. Although Zoom recently responded to these concerns, its response has been criticized as too slow and inadequate.

Early last week, Zoom's failure to quickly quell the concerns snowballed. On Monday, March 30, 2020, New York's attorney general launched an investigation into the company. That investigation demands that Zoom describe the security measures it established to detect hackers and handle increased traffic. It also seeks a broader review of Zoom's security practices and privacy policies. On the same day, Zoom was hit with a consumer class action filed in California, alleging that the company failed to protect users' personal information. *See Cullen v. Zoom Video Communications Inc.,* Civil Action No. 5:20-cv-02155 (N.D. Cal. 2020). Although Zoom responded to initial concerns by updating its privacy policy, it has not placated its critics.

There are several lessons to learn from Zoom's conduct. Businesses, particularly tech businesses, should consider implementing the following in our remote work climate:

- Regularly update privacy policies to address new vulnerabilities.
- Routinely disclose to users what, if any, personal information may be shared with third parties, and how they can opt-out of such information sharing. California's Consumer Privacy Act, for example, now mandates such transparency, and the state's attorney general has reportedly stated that he will not delay enforcement of the Act.

- Re-examine, update, and remind employees of security policies.
- Determine whether end-to-end encryption is possible for the particular application.
- If using Zoom or other similar apps, use the most up-to-date version (which has the latest security features—Zoom removed the controversial remote web server).
- Consider publishing regular transparency reports, which disclose how users' data is shared with federal, state and local governments.

In a time when so much is uncertain, consumers are demanding more transparency from tech companies that hold their personal information, and regulators are listening. Those companies should seek to do more for their users, building trust and strong relationships that extend past the current pandemic.

For additional information, please contact:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cyberecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

Lisa Casey Spaniel, Philadelphia Office
Partner and Co-Chair, Intellectual Property & Technology
215.569.5337 | casey@blankrome.com

Shaun J. Bockert, Philadelphia Office
Associate, Intellectual Property & Technology
215.569.5763 | sbockert@blankrome.com

Jillian M. Taylor, Philadelphia Office
Associate, Intellectual Property & Technology
215.569.5576 | jmtaylor@blankrome.com